Listing of Claims:

CLAIMS

1. (Currently amended) A method for detecting attacks on a data communications network having a plurality of addresses for assignment to data processing systems in the network, the method comprising:

identifying data traffic on the network originating at any assigned address and addressed to any unassigned address, said unassigned address is an address which is free and not assigned to user systems;

inspecting any data traffic so identified for data indicative of an attack; and, on detection of data indicative of an attack, generating an alert signal, wherein the step of inspecting comprises spoofing replies to requests contained in the data traffic identified;

on generation of the alert signal, rerouting any data traffic originating at the address assigned to the data processing system originating the data indicative of the attack to a disinfection address on the network;

on generation of the alert signal, sending an alert message to the disinfection address;

wherein the alert message comprises data indicative of the attack detected.

on receipt of the alert message, sending a warning message from the disinfection address to the address assigned to the data processing system originating the data indicative of the attack;

including in the warning message program code for eliminating the attack when executed by the data processing system originating the data indicative of the attack;

supporting an entity in the handling of the detected attack by one of providing instructions for use of, assistance in executing, and execution of disinfection program code;

providing a report to said entity containing information related to one of alert, disinfection, rerouting, logging, discarding of data traffic in the context of a detected attack;

billing said entity for the execution of at least one of the steps of this method, the charge being billed determined in dependence of one of the size of the network, the number of unassigned addresses monitored, the number of assigned addresses monitored, the volume of data traffic inspected, the number of attacks identified, the number of alerts generated, the signature of the identified attack, the volume of rerouted data traffic, the degree of network security achieved, the turnover of said entity, and

providing said steps of identifying, inspecting and generating to a plurality of entities and using technical data derived from the attack-handling for one of said entities for the attack-handling for another of said entities, wherein the alert message comprises data indicative of the attack detected.

2. - 20. (Canceled)